DETAILED ACTION

1. This is in response to the arguments filed on 21 February 2007.

2. Claims 1-5, 7-9, 11-13 and 15-17 are pending in the application.

3. Claims 1-5, 7-9, 11-13 and 15-17 have been allowed.

4. Claims 6, 10 and 14 have been canceled.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John Vodopia on 19 April 2007.

The application has been amended as follows:

Claim 1 (Amended) A method of providing anonymous digital cash, the method comprising:

providing an entity with a secure co-processor;

a user establishing a secure channel to a program running on said coprocessor;

the user sending an unsigned coin to be digitally signed to the coprocessor using any secure digital signature algorithm; and

said co-processor forming a copy of the unsigned coin;

signing the unsigned coin with a non-homomorphic signature; and

said co-processor ~~forming an encrypted copy of~~ encrypting the signed coin and ~~an encrypted~~ encrypting the copy of the unsigned coin using a public key of a given encryption scheme having said public key and a private key;

sending back to the user both the encrypted copy of the signed coin and the encrypted copy of the unsigned coin, the user having the private key of said given encryption scheme, wherein the user then using said private key to decrypt both the signed and unsigned copies of the coin, and using the pair of signed and unsigned copies of the coin as a unit as digital cash for payment to a recipient while keeping the identity of the user unknown to the coprocessor.

Claim 2 (Amended) A method according to Claim 1, further comprising the steps of:

the processor providing a signature to authenticate;

the user using said encrypted signed coin for payment to a merchant; and

the merchant returning the encrypted signed coin to the entity for credit to an account of the merchant.

Claim 3 (Amended) A method of creating and managing electronic cash, comprising the steps:

a customer communicating to a secure cryptography generator of a bank (i) a given encryption scheme having a public key and a private key, and a (ii) cash amount;

establishing ~~a~~ an unsigned unit representing the cash amount and a copy of the unsigned unit;

signing the unsigned unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to ~~the~~ a coprocessor;

the bank using the secure cryptography generator to encrypt ~~both the~~ a signed unit and the copy of the unsigned unit using the public key of said given encryption scheme;

storing in a database the encrypted signed unit and a value for the unit;

transmitting back to the customer ~~both the~~ an encrypted copy of the signed unit and ~~the~~ an encrypted copy of the unsigned unit;

the customer using the private key of said given encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit;

said customer using the decrypted pair of signed and unsigned copies of the coin as a unit as a payment to a recipient; and

said recipient presenting the pair of signed and unsigned copies of the coin to the bank for credit.

Claim 4 (Amended) A method according to Claim 3, further including the steps of:

establishing an expiration date for the signed encrypted unit; and

storing the expiration date in the database.

Claim 7 (Amended) A system for creating and managing electronic cash, comprising the steps:

a secure cryptography generator, including means for receiving from a customer (i) a cash amount, and (ii) a given encryption scheme having a public key and a private key;

means for establishing a unit representing the cash amount and an unsigned copy of the unit;

means for signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to ~~the~~ a coprocessor;

wherein the secure cryptography generator encrypts both the signed unit and the unsigned copy of the unit using the public key of said given encryption scheme;

a database for storing the encrypted signed unit and a value for the unit;

means for transmitting back to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit;

means for the customer using the private key of the given encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit, wherein the customer then uses the pair of the signed and unsigned copies of the coin as a unit as a payment to a recipient.

Claim 8 (Amended) A system according to Claim 7, further including means for establishing an expiration date for the signed encrypted unit, and wherein the expiration date is stored in the database.

Claim 11 (Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for creating and managing electronic cash, said method steps comprising:

using a secure cryptography generator of a bank to receive from a customer (i) a given encryption scheme having a public key and a private key, and (ii) a cash amount;

establishing ~~a~~ an unsigned unit representing the cash amount and a copy of the unsigned unit;

signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to ~~the~~ a coprocessor;

using the secure cryptography generator to encrypt ~~both the~~ ~~a~~ signed unit and the copy of the unsigned unit using the public key of said given encryption scheme;

storing in a database the encrypted signed unit and a value for the unit;

transmitting back to the customer ~~both the~~ an encrypted copy of the signed unit and ~~the~~ an encrypted copy of the unsigned unit;

the customer using the private key of said given encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit;

the customer using decrypted pair of the signed and unsigned copies of the coin as a unit as a payment to a recipient; and

the recipient presenting the pair of signed and unsigned copies of the coin to the bank for credit.

Claim 12 (Amended) A program storage device according to Claim 11, wherein said method steps further include the steps of:

establishing an expiration date for the signed encrypted unit;

storing the expiration date in the database.

Claim 15 (Amended) A method according to Claim 2, wherein:

the communicating step includes the step of the customer sending to the generator the public key of the encryption scheme; and

the step of using the secure cryptography generator includes the step of using the public key to encrypt the signature on the ~~unit~~ signed coin.

Claim 16 (Amended) A method according to Claim 15, wherein:

the signing step includes the step of using a non-homomorphic signature scheme to sign the ~~unit~~ coin;

the non-homomorphic signature scheme includes a private key and a public key; and

the step of using the non-homomorphic signature scheme includes the step of using the private key of the non-homomorphic signature scheme to sign the ~~unit~~ coin.

Allowable Subject Matter

6. Claims 1-5, 7-9, 11-13 and 15-17 are allowed.

The following is an examiner's statement of reasons for allowance:

As explained in detail in the present application, the instant invention provides a procedure to create and to use electronic cash. With a preferred embodiment of the invention, a customer sends to a bank a request for digital cash and a public key of an encryption scheme of the customer. The bank signs the cash using a secret key of the bank's own digital signature scheme, and encrypts the signature by using the public key provided by the customer. The bank also encrypts, using the public key given to the bank by the customer, an unsigned copy of the cash. A copy of the encrypted signed cash and a copy of the encrypted unsigned cash are both sent to the customer by the bank.

The customer then decrypts both of these copies. That is, both the signed and unsigned copies of the cash by using the private key of the customer's encryption scheme. The customer then uses this decrypted, signed and unsigned pair of copies for payment to a third party. The third party, using these decrypted signed and unsigned copies of the cash, can then ask the bank to confirm the validity of the digital cash. If that validity is confirmed, this third party is able to redeem the digital cash for payment.

An important feature of the present invention is that the bank encrypts both the signed and unsigned copies of the digital cash using the public key of the customer's encryption scheme. That is, the customer has the private key of that encryption scheme. Then, both encrypted copies (the encrypted copy of the signed coin and the encrypted copy of the unsigned coin) are sent back to the customer. Because of this feature, the customer, and only the customer, is able to

decrypt both the signed and unsigned copies of the digital cash by using the private key of the customer's encryption scheme. In this way, only the customer is able to control the use of these copies.

The closest prior art to the current application was Curry et al U.S. Patent No. 6,237,095 B1 (hereinafter Curry). In particular, Curry describes an electronic module used for secure payment, and is particularly directed to communicating encrypted information between the module (preferably portable), and a service provider's equipment. The module has a unique identification capable of creating a random number, e.g., a SALT, and passing the random number along with a request to exchange money to a service provider's equipment. The service provider's equipment encrypts the random number with a public of private key, and along with other information passes the encrypted information to the module as a signed certificate. The module decrypts the certificate and compares the encrypted number with the original random number, where if the same, the procedure is deemed secure. The module may time stamp and store information in memory relating to the transaction. Curry does not disclose sending these two encrypted coins/certificates back to the payee/user. Curry shows that only a money amount and SALT are encrypted and sent as a signed certificate/coin to the payee/user. There is no teaching, though, of sending encrypted copies of two coins/certificates, one signed by the bank and one unsigned by the bank to the user.

In particular, the problem addressed by Curry at lines 8-43 of col. 8 concerns "replay" or "duplication" of digital certificates representing cash. Curry states that a receiver of a payment must take special steps to insure that the digital certificate he receives is not a replay of a previously issued certificate. Curry discloses that the method is a SALT method, whereby a

random number is sent and used in a challenge/response mode. That is, the other party is challenged to return the random number sent as part of that party's response. The payer or bank constructs a signed certificate, which includes both the money amount and the payee's SALT. The payee or user decrypts the signed certificate upon receipt, and confirms that the SALT is the same as was provided. Only the signed certificate is encrypted and returned to the user/payee by the bank/payer. Nowhere does the cited Curry text teach or suggest that the payer/bank sends both an encrypted signed certificate and an encrypted unsigned certificate, as do each of applicants' independent claims 1, 3, 7 and 11, and the claims which depend therefrom.

Independent Claims 1, 3, 7 and 11 clearly describe important features of this invention that are not shown in or suggested by Curry. In particular, Claims 1 and 7 describe the features that encrypted copies of the signed and unsigned coins are encrypted using the public key of an encryption scheme, that both of these copies are sent back to the user or customer, and that the user or the customer uses the private key of this encryption scheme to decrypt both the signed and unsigned copies of the coin. Claims 1 and 7 also describe the feature that the user or customer uses that pair of coins (the signed and unsigned copies of the coin) as digital cash. Claim 7 add the further limitation that this pair of coins is used as a payment to a recipient.

Claims 3 and 11, as presented herein, describe the features that the secure cryptography generator encrypts both the signed unit and the unsigned unit using the public key of the given encryption scheme communicated to the cryptography generator from the customer. As further described in these claims, this pair of encrypted coins are transmitted back to the customer, decrypted by the customer, and used as a unit as payment to a recipient, and this recipient then presents this pair of coins to the bank for credit.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest encrypting the pair of coins, or this use of the pair of subsequently decrypted signed and unsigned coins, as described in claims 1, 3, 7 and 11.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431